Soluciones contra los fraudes de suplantación de personalidad

J. VEGA

Socio de Diversid

OPINION

Diversid Consultoría es una empresa española con vocación de innovación en el área de la autenticación. Sus soluciones de autenticación, dirigidas a la eliminación de las amenazas electrónicas basadas en la suplantación de personalidad (*phishing*/*pharming*, ataques de contraseñas, ...), se fundamentan en la patente europea que comercializa con la que, gracias al uso de claves no reutilizables, conocidas como "**One Time Password**" (OTP), se eliminan estos tipos de fraude que tanto están perjudicando los intereses de consumidores y empresas en todo el mundo.

La filosofía que sigue Diversid es la de que "prevenir es mejor que curar y, por lo tanto, evitar el fraude es mejor que perseguirlo una vez realizado". Para ello propone:

- Un sistema de autenticación para el control de acceso basado en el Intercambio de tres claves OTP que consigue accesos sin posibilidad de fraudes de suplantación de personalidad, como el Phishing, y evitando la denegación de servicio.

- Un sistema para la confirmación de operaciones con Intercambio de tres claves OTP, haciendo uso de dos canales de comunicación diferentes para dicho intercambio, con lo que se consigue eliminar la posibilidad de modificación fraudulenta de datos aplicando la técnica del Man In the Middle.

La aplicación de estas soluciones en un sistema de autenticación permite eliminar los gastos derivados de los diferentes fraudes de suplantación de personalidad y, como beneficio adicional, ofrece la seguridad psicológica que el usuario necesita para aumentar la demanda del uso de este tipo de transacciones no presenciales.

Todos sabemos de la crisis económica por la que estamos pasando y nadie se salva de verse afectado, directa o indirectamente, por ella. La utilización de Internet no puede ser una excepción.

Así, se puede ver que cada vez son más el número de delincuentes que recurren a fraudes por Internet para poder rehacer su economía y para ello van evolucionando tecnológicamente sorprendiendo con nuevos trucos que les permite superar los últimos obstáculos que les hemos ido poniendo.

Mientras tanto, las empresas que ofrecen sus servicios por la red restringen sus presupuestos en seguridad alegando que se tiene que ahorrar. Con ésta política están dejando la vía libre a los defraudadores que indudablemente la aprovecharan para realizar nuevas inversiones, con desarrollos cada vez más creativos, que les permitan mejorar su margen de beneficios. Es como si el papel emprendedor y creativo que normalmente se asocia a un buen empresario se hubiera cedido a los delincuentes.

Parece que las empresas olvidan que la forma más sencilla de conseguir un ahorro es evitar los fraudes. Tomando esta decisión, e invirtiendo en ella, no sólo van a conseguir una disminución de gastos por el ahorro en el fraude sino que también van a marcar una diferencia respecto a sus competidores mejorando su imagen frente al cliente y aumentando su confianza en sus sistemas lo que indudablemente repercutirá en un incremento del número de operaciones realizadas y, también, un incremento de su cuota de mercado dando como resultado un incremento del beneficio.

En relación con este tema del fraude nos encontramos noticias con afirmaciones como:

- Una página cargada bajo SSL cuyo certificado digital provenga de una entidad de confianza (que el navegador cargue sin emitir errores) y en la que aparezca el famoso 'candado' NO puede ser considerada segura.

- La firma digital NO es la 'herramienta definitiva' contra el fraude.

- La falta de formación y descuido del usuario permite el fraude online incluso con firma digital y SSL.

- La confianza en Internet ha comenzado a perderse por efecto del fraude y el robo de identidad.

- Ciberespías y asociaciones crimi-

nales armadas con programas especiales, que roban información digital a empresas, generaron en 2008 pérdidas por un billón de dólares.

Está claro que tenemos un problema importante, económico y social, como consecuencia de un deficiente control de identidad en operaciones realizadas usando canales no presenciales (cajeros automáticos, TPV, fraudes a través de la red, ...).

¿No compensa hacer un esfuerzo que evite esta enorme cifra de fraude que, a la larga, pagamos todos?.

¿Vamos a dejar que se ralentice el uso de una herramienta tan útil como es Internet por culpa del uso de técnicas de identificación de usuarios que ya se han quedado obsoletas y superadas por las técnicas de los delincuentes?

Las empresas, generalmente justificándose con argumentos de tipo comercial, siguen diciendo que no se pueden aplicar técnicas de autenticación que impliquen una incomodidad a sus clientes y puedan ser causa de una huida de clientes a otras empresas de la competencia.

Sobre este tema es conveniente que las empresas sepan que ya en el año 2007 las encuestas realizadas a usuarios de banca online indicaban que el 91% de los titulares de cuentas bancarias encuestados estaban dispuestos a utilizar un nuevo método de autenticación más allá del estandarizado método de "usuario y contraseña". Según esto no parece que los miedos argumentados por las empresas estén realmente justificados y, como consecuencia, no se puede justificar el fraude por razones de una mal entendida "comodidad" del Cliente.

Como agravante en el uso de técnicas de identificación basadas en una clave fija tenemos el hecho de que, según una reciente encuesta online realizada durante el mes de marzo a 676 usuarios de Internet, resulta que el 33% de los internautas todavía utilizan la misma contraseña para todos sus accesos web.

Está claro que estos métodos de usuario y contraseña ya no pueden ser considerados como efectivos pues su validez está claramente superada por las técnicas que son utilizadas por los delincuentes.

¿Es que no hay ningún método de identificación segura de los usuarios? Lo cierto es que ya existen muchas técnicas cuya finalidad es la evitación de fraudes en la red pero es evidente que o no son definitivas o son poco utilizadas pues, como vemos, el fraude sigue existiendo.

TABLA COMPARATIVA DE TÉCNICAS DE AUTENTICACIÓN PREVENTIVAS

Técnica antifraude **VS** *Técnica de fraude*	**Phishing diferido**	**Phishing en tiempo real**	**Modificación on line de datos (Man in the Middle, Troyanos,...)**
Certificado electrónico	Lo evita	Lo evita	No lo evita (1)
Autenticación con tarjeta de coordenadas	No lo evita (2)	Lo evita	No lo evita
Una clave OTP	Lo evita con condiciones	No lo evita	No lo evita
Dos claves OTP	Lo evita con condiciones	No lo evita	No lo evita
Una clave fija y dos OTP (3)	Lo evita	Lo evita	No lo evita
Tres claves OTP	Lo evita	Lo evita	No lo evita

SOLUCIÓN DE DIVERSID

(1) En una máquina controlada por un troyano no se puede tener seguridad de qué se está firmando.

(2) Si en un proceso de phishing, o con un troyano, un defraudador se hace con una de nuestras claves de la tarjeta, ¿cómo podemos evitar que a base de reiterados intentos de operar llegue el caso de que la clave solicitada por el banco coincida con la que tiene el defrau.dador?.

(3) Al utilizar una primera clave con valor fijo será fácil que un atacante pueda hacerse con ella y, enviándola de forma repetida y continuada, puede llegar a conseguir una denegación de servicio.

TABLA COMPARATIVA DE TÉCNICAS DE AUTENTICACIÓN REACTIVAS

Técnica antifraude VS Técnica de fraude	Phishing diferido	Phishing on tiempo real	Modificación on line de datos (Man in the Middle, Troyanos,...)
Servicios antiphishing	Lo evita después de ser detectado (4)	Lo evita después de ser detectado (4)	No lo evita
Antitroyanos	Lo evita después de ser detectado (5)	Lo evita después de ser detectado (5)	Lo evita después de ser detectado (5)

(4) Estudios revelan que durante las 6 primeras horas de un ataque de Phishing se llegarían a concentrar el 51,6% de las visitas mientras que los servicios antiphishing reactivos mantienen medias superiores a las 6 horas de cierre.

(5) Pueden pasar días, o incluso semanas, hasta que un troyano llega por primera vez a un laboratorio antivirus.

TABLA COMPARATIVA DE LA EFECTIVIDAD DE TÉCNICAS ANTIFRAUDE PARA LA CONFIRMACIÓN DE OPERACIONES SENSIBLES

Técnica antifraude VS Técnica de fraude	Phishing diferido	Phishing en tiempo real	Modificación on line de datos (Man in the Middle, Troyanos,...)
Acceso con clave fija y confirmación de operaciones con clave fija y SMS con clave OTP (6)	No evita la consulta	No evita la consulta	Lo evita
Acceso con tres claves OTP y confirmación de operaciones con clave fija y SMS con clave OTP (6)	Lo evita	Lo evita	Lo evita
Acceso con tres claves OTP y confirmación de operaciones con tres claves OTP y dos canales de comunicación ***SOLUCIÓN DE DIVERSID***	Lo evita	Lo evita	Lo evita

(6) Al utilizar una clave con valor fijo será fácil que un atacante pueda hacerse con ella y, enviándola de forma repetida y continuada, puede llegar a conseguir una denegación de servicio además de una mala imagen de la entidad al llegarle al cliente los SMS de operaciones que él no ha solicitado.

Para tener una visión de conjunto utilicemos un cuadro que nos permita comparar la efectividad de las técnicas antifraude más conocidas frente a los fraudes más frecuentes.

Empecemos valorando primero las técnicas orientadas a garantizar la autenticación de los usuarios para posteriormente hacer lo mismo con las usadas para la confirmación de operaciones.

Dentro de las primeras con encontramos con unas soluciones de tipo preventivo y otras de tipo reactivo frente a los ataques que ya se han producido.

Como se ha podido ver en las tablas anteriores ciertamente ya existen soluciones para los más frecuentes fraudes en la operativa por Internet.

Dentro de estas soluciones quiero destacar las suministradas por Diversid que, además de proporcionar una cobertura completa para el Phishing y Man In The Middle, destacan por su sencillez de uso, bajo coste y facilidad de despliegue de la aplicación entre sus usuarios. Algunas de las características a subrayar de las soluciones de autenticación de Diversid son:

- La empresa está obligada a autenticarse ante el cliente.
- El cliente se autentica después de que la empresa se ha autenticado frente al cliente.
- El cliente no tiene que llevar ningún dispositivo nuevo ya que usa su teléfono móvil.
- En su solución de control de acceso no hace uso de SMS y por tanto no depende de la disponibilidad de cobertura.
- El cliente puede darse de alta en el sistema de autenticación sin tener que personarse en la empresa.
- Las OTP que se usan son independientes de la variable temporal y no tienen el problema de caducidad por tiempo.
- Están almacenadas por lo que elimina los requerimientos de incremento de la capacidad de procesamiento necesaria en los casos de generación de las OTP en modo online y también posibles ataques que provoquen una denegación de servicio.

Son los responsables de decidir cómo deben ser los sistemas de sus empresas los que han de dar el paso de aplicar nuevos sistemas de autenticación, como las soluciones de Diversid, potenciando la seguridad del cliente frente a la mal entendida "comodidad" del cliente.

Sin olvidar la diferencia que existe ante la posible gravedad de las consecuencias, podemos decir que al igual que para viajar en moto es obligatorio hacerlo con el casco puesto, también es cierto que, para "viajar" por Internet es necesario hacer uso de procedimientos seguros. ■